Priority-Based Virus Scanning With Priorities Based At Least In Part On Heuristic Prediction Of Scanning Risk

ABSTRACT

Anti-virus scanners can be deliberately disabled, inadvertently disabled, or simply slowed down to a point where the scanner becomes ineffective and the primary function of the scanning host device is disrupted when a suitably complex file is received by the scanning system for scanning. Archive files pose particular problems for scanners, since archives may contain very complex data structures, and require time consuming analysis. Virus scanners typically scan each element of an archive. Some virus scanners decompress each archive component for scanning. Virus developers have taken advantage of this scanning approach by creating complex archives designed to overwhelm a scanner, leaving a system unprotected or in a denial of service state. To counter such measures, when an archive (or other file) is passed to a scanner, various heuristics are applied to the archive so as to determine a risk-based scanning priority for the archive. Priorities can include normal priority, low priority for archives having suspicious characteristics, and discard without scanning for archives appearing to be constructed so as to overwhelm a scanner. Normal priority scans can occur immediately, while low priority scans can be relegated to only occurring while the scanning system is otherwise idle.